(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－249921

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　11/10	３３０	Ｇ０６Ｆ　11/10	３３０Ｑ

審査請求　未請求　請求項の数５　ＯＬ　（全９頁）

(21)出願番号　特願平10－53236

(22)出願日　平成10年(1998)３月５日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　花木　義孝
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　滝本　智之　（外１名）

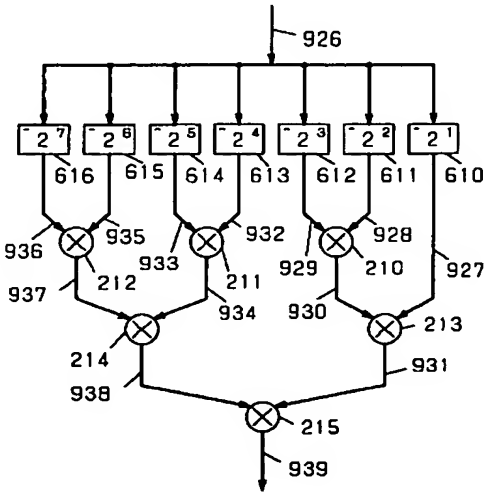
(54)【発明の名称】　ガロア体演算器

(57)【要約】

【課題】　ガロア体上の逆元の生成を行うガロア体演算器を実現するにあたり、高速なパイプライン動作を実現しつつ、回路規模の小さなガロア体演算器を実現することを目的とする。

【解決手段】　入力信号をガロア体ベキ乗算回路６１０～６１６に入力し、それぞれ２乗～１２８乗のベキ乗算をした出力をガロア体乗算器２１０～２１５からなるツリーで互いに掛け合わせ、入力の逆元を得る。

210~215　ガロア体乗算器
610　ガロア体２乗回路
611　ガロア体４乗回路
612　ガロア体８乗回路
613　ガロア体１６乗回路
614　ガロア体３２乗回路
615　ガロア体６４乗回路
616　ガロア体１２８乗回路



【特許請求の範囲】

【請求項１】　ガロア体２の１乗々回路～ガロア体２の（ｎ－１）乗々回路と、ツリー状に接続されたｎ－２個のガロア体乗算器とで構成され、ガロア体ＧＦ（２＾ｎ）上の逆元を生成することを特徴とするガロア体演算器。

【請求項２】　個々のガロア体２の１乗々回路～ガロア体２の（ｎ－１）乗々回路およびツリー状に接続されたｎ－２個のガロア体乗算器の、すべてまたはその一部を、それぞれ独立したガロア体２の定数乗々回路およびガロア体乗算器として使用するための選択手段を有することを特徴とする請求項１記載のガロア体演算器。

【請求項３】　ガロア体２の１乗々回路～ガロア体２の（ｎ－１）乗々回路と、ツリー状に接続されたｎ－１個のガロア体乗算器とで構成され、ガロア体ＧＦ（２＾ｎ）上の除算を実行することを特徴とするガロア体演算器。

【請求項４】　個々のガロア体２の１乗々回路～ガロア体２の（ｎ－１）乗々回路およびツリー状に接続されたｎ－１個のガロア体乗算器の、すべてまたはその一部を、それぞれ独立したガロア体２の定数乗々回路およびガロア体乗算器として使用するための選択手段を有することを特徴とする請求項３記載のガロア体演算器。

【請求項５】　ガロア体２の１乗々回路～ガロア体２の（ｎ－１）乗々回路と、ツリー状に接続されたｎ－１個のガロア体乗算器と、個々の前記ガロア体２の１乗々回路～ガロア体２のｎ－１乗々回路およびツリー状に接続されたｎ－１個の前記ガロア体乗算器の、すべてまたはその一部を、それぞれ独立したガロア体２の定数乗々回路およびガロア体乗算器として使用するための選択手段と０個以上のガロア体乗算器と、演算途中のデータを保持するレジスタとで構成され、ガロア体上の多項式の除算をおこなうことを特徴とするガロア体演算器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】デジタルＡＶシステムや情報通信などの分野において、誤り訂正符号に関する技術の応用が盛んである。本発明は、誤り訂正符号として有力なリード・ソロモン符号の復号・符号化をおこなうためのガロア体演算器に関するものである。

【０００２】

【従来の技術】従来、ガロア体ＧＦ（２＾ｎ）上の逆元生成器は、逆元ＲＯＭと呼ばれるＲＯＭによって構成されていた。逆元ＲＯＭには、アドレス入力に対してガロア体上の逆元が出力されるようにデータが格納されている。

【０００３】図５に、従来のガロア体上の逆元生成器の構成を示す。同図において、１２０は逆元ＲＯＭ、９００、９０１は信号線である。

【０００４】図５の構成によるガロア体逆元生成器の動作を、以下に説明する。まず、ガロア体演算器への入力が、信号線９００を介して、逆元ＲＯＭ１２０に入力され、その逆元が逆元ＲＯＭ１２０から出力され、信号線９０１を介してガロア体演算器から出力される。

【０００５】図６に、従来のガロア体除算器の構成を示す。同図において、１３０は逆元ＲＯＭ、２３０はガロア体乗算器、９０２、９０３、９０４、９０５は信号線である。

【０００６】図６の構成によるガロア体除算器の動作を、以下に説明する。まず、ガロア体除算器へ除数として与えられた入力が、信号線９０２を介して、逆元ＲＯＭ１３０に入力され、その逆元が逆元ＲＯＭ１３０から出力され、信号線９０３を介して、ガロア体乗算器２３０に入力される。また、ガロア体除算器へ被除数として与えられた入力が、信号線９０４を介して、ガロア体乗算器２３０に入力される。ガロア体乗算器２３０では、除数の逆元と被除数を乗ずることによってガロア体除算の結果が生成され、信号線９０５を介して、ガロア体除算器から出力される。従来の構成では、以上のようにして、ガロア体除算器を得ていた。

【０００７】図７は、従来のガロア体多項式除算器の構成を示すブロック図である。説明の便宜上、この構成は、ガロア体上の最大３次の除数多項式と最大３次の被除数多項式の除算をおこなうことができるものとしている。図４において、２４０、２４１、２４２はガロア体乗算器、３４０、３４１、３４２はガロア体加算器、４４０はガロア体除算器、５４０、５４１、５４２、５４３、５４４、５４５、５４６、５４７はそれぞれレジスタ、９０６、９０７、９０８、９０９、９１０、９１１、９１２、９１３、９１４、９１５、９１６、９１７、９１８、９１９、９２０、９２１、９２２、９２３、９２４、９２５はそれぞれ信号線である。

【０００８】従来のガロア体多項式除算器の動作を、下記の３ステップに分けて説明する。ただし、商多項式Ｒ（ｘ）は、下記のようにあらわされるものとする。

【０００９】Ｒ（ｘ）＝ｒ＿３ｘ＾３＋ｒ＿２ｘ＾２＋ｒ＿１ｘ＋ｒ＿０

また、初期状態において、レジスタ５４０、５４１、５４２、５４３には、それぞれ被除数となる多項式の０次、１次、２次、３次の係数が格納されており、レジスタ５４４、５４５、５４６、５４７には、それぞれ除数となる多項式の０次、１次、２次、３次の係数が格納されているものとする。除数多項式は、中間剰余多項式の初期値となる。

【００１０】＜ステップ１＞まず、除数多項式の最高次の係数が０以外になるように、除数多項式が正規化される。すなわち、レジスタ５４７の値が０以外になるまで、除数多項式の係数５４０、５４１、５４２、５４３を低次から高次の方向に１次分ずつシフトする。シフトするときに、最低次の係数を格納するレジスタ５４４に

は、値０がシフトインされる。

【００１１】＜ステップ２＞次に、被除数多項式の最高次係数と、正規化された除数多項式の最高次係数との、ガロア体除算がおこなわれる。ガロア体除算の結果として、商多項式の係数が１次分だけ求まる。すなわち、レジスタ５４３の値が信号線９１２を介してガロア体除算器４４０に入力されており、正規化された除数多項式の最高次の係数を格納するレジスタ５４７の値が信号線９１６を介してガロア体除算器４４０に入力されている。ガロア体除算器４４０では、被除数の最高次係数を被除数とし、除数の最高次係数を除数とする除算がおこなわれる。除算結果は、商多項式Ｒ（ｘ）の最高次係数ｒ＿ｄｅｇ（Ｒ（ｘ））として、信号９２５を介して出力される。

【００１２】＜ステップ３＞次に、＜ステップ１＞で正規化された除数多項式の各係数と、＜ステップ２＞で求まった商多項式の１次分の係数とのガロア体乗算をおこない、その結果と、これまでに求まった中間剰余多項式とのガロア体加算をおこなうという、ガロア体積和演算がおこなわれる。ガロア体積和演算の結果は、次の中間剰余多項式となる。すなわち、信号９２５が、ガロア体乗算器２４０、２４１、２４２に入力されている。また、レジスタ５４４、５４５、５４６から、それぞれ除数多項式の０次、１次、２次の係数が、それぞれ信号線９１３、９１４、９１５を介して、それぞれガロア体乗算器２４０、２４１、２４２へ入力されており、ガロア体除算器４４０の出力と乗ぜられ、ぞれぞれ信号９２０、９２１、９２２を介してガロア体加算器３４０、３４１、３４２に入力される。また、レジスタ５４０、５４１、５４２の値がそれぞれ信号線９０６、９０８、９１０を介してガロア体加算器３４０、３４１、３４２に入力され、それぞれ信号線９２０、９２１、９２２の値と加算され、それぞれ信号線９０７、９０９、９１１を介してレジスタ５４１、５４２、５４３に格納される。レジスタ５４０には、値０が格納される。

【００１３】＜ステップ２＞と＜ステップ３＞を繰り返すことによって、＜ステップ２＞が実行されるたびに、商多項式の係数が１次分ずつ、ｒ＿ｄｅｇ（Ｒ（ｘ））、ｒ＿（ｄｅｇ（Ｒ（ｘ））－１）、ｒ＿（ｄｅｇ（ｒ（ｘ））－２）、…、ｒ＿１、ｒ＿０、という順に、信号９２５から出力される。必要があれば、この出力をシリアルーパラレル変換することによって、商多項式を求めることができる。剰余多項式は、＜ステップ２＞でｒ＿０が求まった直後の＜ステップ３＞を実行したときに、レジスタ５４０、５４１、５４２、５４３に格納されている中間剰余多項式として得られる。レジスタ５４０、５４１、５４２、５４３にそれぞれ、０次、１次、２次、３次の係数が得られる。

【００１４】このようにして、従来のガロア体多項式除算器では、＜ステップ１＞除数多項式の正規化と、＜ステップ２＞ガロア体除算および＜ステップ３＞ガロア体積和演算の繰り返しによって、ガロア体多項式除算の結果を得ていた。

【００１５】

【発明が解決しようとする課題】以下に、上記ガロア体演算器の構成における課題について説明する。従来の構成では、ガロア体上の逆元を生成するため、あるいは、ガロア体上の除算を実行するためには、ガロア体上の逆元を記憶したＲＯＭが必要であった。そのため、ガロア体演算器にパイプライン構造をもたせて、ＲＯＭのアクセス速度以上のスループットを実現するには、複数のＲＯＭをインターリーブさせる必要があり、高速なパイプライン動作を実現しつつ回路規模の小さなガロア体演算器を得るのが困難である、という課題があった。また、ガロア体の原始多項式に対応した逆元ＲＯＭが必要であるため、複数の原始多項式に対応するためには、原始多項式の数と同数の逆元ＲＯＭが必要となる。そのため、複数の原始多項式に対応しつつ回路規模の小さなガロア体演算器を得るのが困難である、という課題があった。また、ガロア体上の逆元を記憶するための専用ＲＯＭを実装する必要があるため、ゲートアレイやＦＰＧＡなどに実装するのが困難である、という課題があった。

【００１６】また、従来の構成では、ガロア体除算とガロア体乗算の双方を必要とするガロア体演算器を構成する場合に、ガロア体除算器とガロア体乗算器の双方を実装する必要があり、回路規模が小さなガロア体演算器を構成するのが困難である、という課題があった。

【００１７】また、従来の構成では、最高次数ｍのガロア体上の多項式の除算を実現するには、ガロア体除算器と、ｍ－１個のガロア体乗算器が必要であった。回路規模が大きなガロア体除算器に加えて、ｍ－１個もの多数のガロア体乗算器を持つ必要があるため、回路規模の小さなガロア体上の多項式の除算器を得るのが困難である、という課題があった。また、ガロア体除算器として、ガロア体上の逆元を記憶するためのＲＯＭを持つ前記従来のガロア体除算器を使用するため、従来のガロア体上の除算器についてこれまでに述べた課題のすべてが、従来のガロア体上の多項式の除算器にも当てはまった。

【００１８】本発明は、上記のような従来の課題を解決するものであり、ガロア体上の逆元の生成、あるいは、ガロア体上の除算をおこなうガロア体演算器を実現するにあたり、高速なパイプライン動作を実現しつつ回路規模の小さなガロア体演算器を提供すること、および、複数の原始多項式に対応しつつな回路規模の小さなガロア体演算器を提供すること、および、ゲートアレイやＦＰＧＡなどにも容易に実装可能なガロア体演算器を提供することを目的とする。

【００１９】また、本発明は、ガロア体除算器とガロア体乗算器の双方を含みつつ、回路規模の小さなガロア体

演算器を提供することを目的とする。

【００２０】また、本発明は、ガロア体上の多項式の除算を実現するための、小規模なガロア体演算器を提供することを目的とする。

【００２１】

【課題を解決するための手段】本発明の請求項１記載の、ガロア体上の逆元を生成するガロア体演算器は、ガロア体ＧＦ（２＾ｎ）上において、前記ガロア体演算器の入力をそれぞれ入力とするようなガロア体２の１乗々回路～ガロア体２の（ｎ－１）乗々回路と、前記ガロア体２の１乗々回路～ガロア体２の（ｎ－１）乗々回路の出力すべてを掛けあわせるようにツリー状に接続されたｎ－２個のガロア体乗算器とで構成されることを特徴とする。

【００２２】この構成では、ガロア体ＧＦ（２＾ｎ）上のガロア体演算は、（ｎ－１）個の項の総乗となっている。（ｎ－１）つの項の総乗は、たかだか（ｌｏｇ（ｎ－１））＋１段の乗算器のツリーで構成することが可能である（ただし、対数の底は２。以下同じ）。よって、この構成から、ガロア体上の逆元生成回路を、（ｌｏｇ（ｎ－１））＋１段のパイプラインステージに、容易に分割することができる。

【００２３】さらに、ガロア体乗算器は、回路規模をさほど増大させることなく、対応する原始多項式の数が増大させることが可能である。よって、この構成によれば、複数の原始多項式に対応しつつ、小規模なガロア体演算器を得ることができる。

【００２４】さらに、この構成では、ガロア体演算器全体をランダムロジックで構成することが可能である。よって、ゲートアレイやＦＰＧＡなどにも容易に実装することが可能である。

【００２５】本発明の請求項２記載のガロア体演算器は、請求項１記載のガロア体演算器を構成する、個々のガロア体２の定数乗々回路および（ｎ－２）個のガロア体乗算器の、すべてまたはその一部を、それぞれ独立したガロア体２の定数乗々回路およびガロア体乗算器として使用するための選択手段を有することを特徴とする。

【００２６】この構成によれば、ガロア体の逆元生成器とガロア体乗算器とガロア体２の定数乗乗回路をもつような場合と比較して、回路規模の小さなガロア体演算器を得ることができる。

【００２７】本発明の請求項３記載の、ガロア体上の除算をおこなうガロア体演算器は、ガロア体ＧＦ（２＾ｎ）上において、ガロア体演算器の除数を入力とするガロア体２の１乗々回路～ガロア体２の（ｎ－１）乗々回路と、前記ガロア体２の１乗々回路～ガロア体２の（ｎ－１）乗々回路とガロア体演算器の被除数のすべてを掛け合わせるようにツリー状に接続されたｎ－１個のガロア体乗算器とで構成されることを特徴とする。

【００２８】なお、これはガロア体ＧＦ（２＾ｎ）上の

元ａ、ｂについて、以下の等式が成立するという代数的な性質に基づいている：

ｂ÷ａ＝ｂ×ａ＾（－１）＝ｂ×ａ＾（２＾１）×ａ＾（２＾２）×…×ａ＾（２＾ｎ）

この構成では、前記本発明の請求項１で述べたような、複数段のステージを持つパイプラインに容易に分割することが可能であり、複数の原始多項式に対応しつつ、小規模なガロア体演算器を得ることが可能であり、かつ、ゲートアレイやＦＰＧＡなどにも容易に実装することが可能である、という議論がそのまま当てはまる。

【００２９】本発明の請求項４記載のガロア体演算器は、請求項３記載のガロア体演算器を構成する、個々のガロア体２の定数乗々回路および個のガロア体乗算器の、すべてまたはその一部を、それぞれ独立したガロア体２の定数乗々回路およびガロア体乗算器として使用するための選択手段を有することを特徴とする。

【００３０】この構成によれば、ガロア体の逆元を生成したり、ガロア体の除算を実行する必要がないサイクルに、ガロア体２の定数乗乗回路、および、ガロア体乗算器として、ガロア体演算器を利用することができる。従って、回路規模の小さなガロア体演算器を得ることができる。

【００３１】本発明の請求項５記載のガロア体演算器は、本発明の請求項４のガロア体演算器と、０個以上のガロア体乗算器と、演算途中のデータを保持するレジスタとで構成され、ガロア体上の多項式の除算をおこなうことを特徴とする。

【００３２】すでに従来の技術の欄で述べたように、最高ｍ次のガロア体上の多項式の除算をおこなうには、ガロア体の除算と、相互に並列に実行可能なｍ－１回のガロア体乗算とを、交互に繰り返す必要がある。本発明の請求項５の構成によれば、本発明の請求項４で述べたガロア体ＧＦ（２＾ｎ）上のガロア体演算器をガロア体除算器として使用するサイクルと、独立したｎ－１個のガロア体乗算器として使用するサイクルとを、交互に繰り返すことによって、ガロア体除算をおこなうことが可能である。このとき、ガロア体除算器と、ｍ－１個のガロア体乗算器とを共用することが可能となり、回路規模の小さなガロア体上の多項式の除算器を得ることが可能となる。

【００３３】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しながら説明する。

【００３４】（実施の形態１）まず、本発明の実施の形態１のガロア体演算器について説明する。

【００３５】図１は、本実施の形態１のガロア体演算器の構成を示すブロック図である。図１のガロア体演算器は、ガロア体上の逆元を生成する。説明の便宜上、図１にはガロア体ＧＦ（２＾８）上のガロア体演算器を示している。

【００３６】図１において２１０、２１１、２１２、２１３、２１４、２１５はガロア体乗算器、６１０はガロア体２乗回路、６１１はガロア体４乗回路、６１２はガロア体８乗回路、６１３はガロア体１６乗回路、６１４はガロア体３２乗回路、６１５はガロア体６４乗回路、６１６はガロア体１２８乗回路、９２６、９２７、９２８、９２９、９３０、９３１、９３２、９３３、９３４、９３５、９３６、９３７、９３８、９３９はそれぞれ信号線である。

【００３７】以上のように構成された実施の形態１のガロア体演算器の動作を、以下に説明する。まず、ガロア体演算器の入力が信号線９２６を介してガロア体２乗回路６１０、ガロア体４乗回路６１１、ガロア体８乗回路６１２、ガロア体１６乗回路６１３、ガロア体３２乗回路６１４、ガロア体６４乗回路６１５、ガロア体１２８乗６１６に入力され、それぞれ２乗、４乗、８乗、１６乗、３２乗、６４乗、１２８乗されて、それぞれ信号線９２７、９２８、９２９、９３２、９３３、９３５、９３６を介して、ガロア体乗算器２１０、２１１、２１２、２１３、２１４、２１５からなるガロア体乗算器のツリーで互いに掛け合わせられ、信号線９３９から乗算結果が出力される。この乗算結果は、ガロア体演算器の入力を２乗、４乗、８乗、１６乗、３２乗、６４乗、１２８乗したものを、それぞれ掛け合わせた数となる。これはガロア体演算器の入力の逆元である。

【００３８】（実施の形態２）次に、本発明の実施の形態２のガロア体演算器について説明する。

【００３９】図２は、本実施の形態２のガロア体演算器の構成を示すブロック図である。同図のガロア体演算器は、ガロア体上の除算をおこなう。説明の便宜上、図５にはガロア体ＧＦ（２＾８）上のガロア体演算器を示している。

【００４０】図５において２５０、２５１、２５２、２５３、２５４、２５５、２５６はそれぞれガロア体乗算器、６５０はガロア体２乗回路、６５１はガロア体４乗回路、６５２はガロア体８乗回路、６５３はガロア体１６乗回路、６５４はガロア体３２乗回路、６５５はガロア体６４乗回路、６５６はガロア体１２８乗回路、９４０、９４１、９４２、９４３、９４４、９４５、９４６、９４７、９４８、９４９、９５０、９５１、９５２、９５３、９５４、９５５はそれぞれ信号線である。

【００４１】以上のように構成された実施の形態２のガロア体演算器の動作を、以下に説明する。まず、ガロア体演算器の被除数が信号線９４１を介してガロア体乗算器２５０に入力される。また、ガロア体演算器の除数が信号線９４０を介してガロア体２乗回路６５０、ガロア体４乗回路６５１、ガロア体８乗回路６５２、ガロア体１６乗回路６５３、ガロア体３２乗回路６５４、ガロア体６４乗回路６５５、ガロア体１２８乗６５６に入力され、それぞれ２乗、４乗、８乗、１６乗、３２乗、６４乗、１２８乗されて、それぞれ信号線９４２、９４４、９４５、９４８、９４９、９５１、９５２を介して、ガロア体乗算器２５０、２５１、２５２、２５３、２５４、２５５、２５６からなるガロア体乗算器のツリーに入力され、ガロア体演算器の被除数とともに掛け合わせられ、信号線９５５から乗算結果が出力される。この乗算結果は、ガロア体演算器の被除数、および、除数を２乗、４乗、８乗、１６乗、３２乗、６４乗、１２８乗したものをそれぞれ掛け合わせた数、すなわちガロア体演算器の被除数を除数で割った除算結果である。

【００４２】（実施の形態３）次に、本発明の実施の形態３のガロア体演算器について説明する。

【００４３】図３は、本実施の実施の形態３のガロア体演算器の構成を示すブロック図である。同図のガロア体演算器は、選択信号の値に応じて、ガロア体ＧＦ（２＾m）上のガロア体除算器として動作するか、あるいは、各々独立したガロア体２の１乗乗回路～ガロア体２の（ｍ－１）乗乗回路と複数のガロア体乗算器として動作するかを切り替えることが可能である。説明の便宜上、図３はガロア体ＧＦ（２＾４）上のガロア体演算器の場合について示している。すなわち、同図において、ｍ＝４である。

【００４４】図３において、２６０、２６１、２６２はガロア体乗算器、６６０はガロア体２乗回路、６６１はガロア体４乗回路、６６２はガロア体８乗回路、７６０、７６１、７６２、７６３、７６４、７６５、７６６はセレクタ、９５６、９５７、９５８、９５９、９６０、９６１、９６２、９６３、９６４、９６５、９６６、９６７、９６７、９６８、９６９、９７０、９７１、９７２、９７３、９７４、９７５、９７６、９７７、９７８はそれぞれ信号線である。９７９は選択信号の加わる信号線である。

【００４５】以上のように構成された実施の形態３のガロア体演算器の動作を以下に説明する。まず、信号線９７９に加わる選択信号が１である場合について説明する。このとき、図６のガロア体演算器は、ガロア体除算器として動作する。まず、ガロア体除算の被除数が信号線９５６を介して、セレクタ７６０、７６１、７６２に入力され、選択信号が１であるので選択・出力され、信号線９５７、９６０、９６３を介して、ガロア体２乗回路６６０、ガロア体４乗回路６６１、ガロア体８乗回路６６２に入力される。ガロア体除算の被除数を２乗、４乗、８乗した値が、それぞれガロア体２乗回路６６０、ガロア体４乗回路６６１、ガロア体８乗回路６６２から出力され、それぞれ信号線９５８、９６１、９６４を介してセレクタ７６７、７６４、７６５に入力され、選択信号が１であるので選択・出力され、それぞれ信号線９８０、９６２、９６５を介して、ガロア体乗算器２６１、２６０、２６０へ入力される。また、ガロア体除算の除数が信号線９７６を介してガロア体乗算器９６１に

入力される。選択信号が１であるとき、ガロア体乗算器２６０、２６１、２６２はガロア体乗算のツリーを構成している。これまでの動作でガロア体除算の被除数の２乗、４乗、８乗、およびガロア体除算の除数がガロア体乗算のツリーに入力されており、これらを掛け合わせた値、すなわちガロア体除算の結果が信号線２６２を介して出力される。

【００４６】次に、信号線９７９に加わる選択信号が０である場合、図３に示したガロア体演算器は、各々１個のガロア体２乗回路、ガロア体４乗回路、ガロア体８乗回路、および３個のガロア体乗算器として動作する。

【００４７】（実施の形態４）次に、本発明の実施の形態４のガロア体演算器について説明する。

【００４８】図４は、本発明の実施の形態４のガロア体演算器の構成を示すブロック図である。同図のガロア体演算器は、図７で示したガロア体多項式除算器の構成において、ガロア体除算器４４０および３個のガロア体乗算器２４０、２４１、２４２を、発明の実施の形態３で述べた図３で示したガロア体演算器で置き換え、かつガロア体除算の結果を格納するためのレジスタを追加した構成をしている。本発明の実施の形態４のガロア体多項式除算器の動作を、下記の３ステップに分けて説明する。ただし、商多項式Ｒ（ｘ）は、下記のようにあらわされるものとする。

【００４９】Ｒ（ｘ）＝ｒ＿３ｘ＾３＋ｒ＿２ｘ＾２＋ｒ＿１ｘ＋ｒ＿０

また、初期状態において、レジスタ５７０、５７１、５７２、５７３には、それぞれ被除数となる多項式の０次、１次、２次、３次の係数が格納されており、レジスタ５７４、５７５、５７６、５７７には、それぞれ除数となる多項式の０次、１次、２次、３次の係数が格納されているものとする。除数多項式は、中間剰余多項式の初期値となる。

【００５０】＜ステップ１＞まず、除数多項式の最高次の係数が０以外になるように、除数多項式が正規化される。すなわち、レジスタ５７７の値が０以外になるまで、除数多項式の係数５７０、５７１、５７２、５６３を低次から高次の方向に１次分ずつシフトする。シフトするときに、最低次の係数を格納するレジスタ５７４には、値０がシフトインされる。

【００５１】＜ステップ２＞次に、本発明の実施例を構成する本発明の実施の形態３で述べたガロア体演算器がガロア体除算器として動作するような値が選択信号に印加され、被除数多項式の最高次係数と、正規化された除数多項式の最高次係数との、ガロア体除算がおこなわれる。ガロア体除算の結果として、商多項式の係数が１次分だけ求まる。また、ガロア体除算の結果は、レジスタに記憶され、＜ステップ３＞での利用に備えられる。すなわち、選択信号１００５には、値１が印可され、セレクタ７７０、７７１、７７２、７７３、７７４、７７５、７７６に入力される。これによって、本発明の実施の形態３で述べたガロア体演算器４７０は、ガロア体除算器として動作する。また、レジスタ５７３の値が信号１００３を介してガロア体演算器４７０に入力されており、正規化された除数多項式の最高次の係数を格納するレジスタ５７７の値が信号９９１とセレクタ７７０を介してガロア体演算器４７０へ入力されている。ガロア体演算器４７０では、被除数の最高次係数を被除数とし、除数の最高次係数を除数とする除算がおこなわれる。除算結果は、商多項式Ｒ（ｘ）の最高次係数ｒ＿ｄｅｇ（Ｒ（ｘ））として、信号線１００１を介して出力される。また、ｒ＿ｄｅｇ（Ｒ（ｘ））の値は、レジスタ５７８に格納され、＜ステップ３＞での利用に備えられる。

【００５２】＜ステップ３＞次に、本発明の実施例を構成する、本発明の実施の形態３で述べたガロア体演算器が３個のガロア体乗算器として動作するような値が選択信号に印加され、＜ステップ１＞で正規化された除数多項式の各係数と、＜ステップ２＞で求まった商多項式の１次分の係数とのガロア体乗算をおこない、その結果と、これまでに求まった中間剰余多項式とのガロア体加算をおこなうという、ガロア体積和演算がおこなわれる。ガロア体積和演算の結果は、次の中間剰余多項式となる。すなわち、信号線１００５に加わる選択信号に値０が印加される。これによって、本発明の実施の形態３で述べたガロア体演算器４７０は、３個のガロア体乗算器として動作する。次に、＜ステップ２＞で求まったレジスタ５７８の値が信号線１００２と、セレクタ７７５、７７４、７７２を介して、それぞれガロア体乗算器２７０、２７１、２７２に入力されている。また、レジスタ５７４、５７５、５７６から、それぞれ除数多項式の０次、１次、２次の係数が、それぞれ信号線９８８、９８９、９９０を介して、それぞれガロア体乗算器２７０、２７１、２７２へ入力されており、レジスタ５７８の出力と乗ぜられ、ぞれぞれ信号線１００１、１００６、１００７を介してガロア体加算器３７０、３７１、３７２に入力される。また、レジスタ５７０、５７１、５７２の値がそれぞれ信号線９８２、９８４、９８６を介してガロア体加算器３７０、３７１、３７２に入力され、それぞれ信号線１００１、１００６、１００７の値と加算され、それぞれ信号線９８３、９８５、９８７を介してレジスタ５７１、５７２、５７３に格納される。レジスタ５７０には、値０が格納される。

【００５３】＜ステップ２＞と＜ステップ３＞を繰り返すことによって、＜ステップ２＞が実行されるたびに、商多項式の係数が１次分ずつ、ｒ＿ｄｅｇ（Ｒ（ｘ））、ｒ＿（ｄｅｇ（Ｒ（ｘ））－１）、ｒ＿（ｄｅｇ（ｒ（ｘ））－２）、…、ｒ＿１、ｒ＿０、という順に、信号１００１から出力される。必要があれば、この出力をシリアルーパラレル変換することによって、商

11

多項式を求めることができる。剰余多項式は、＜ステップ２＞でｒ＿０が求まった直後の＜ステップ３＞を実行したときに、レジスタ５７０、５７１、５７２、５７３に格納されている中間剰余多項式として得られる。レジスタ５７０、５７１、５７２、５７３にそれぞれ、０次、１次、２次、３次の係数が得られる。

【００５４】このようにして、本発明の実施の形態４のガロア体多項式除算器では、＜ステップ１＞除数多項式の正規化と、＜ステップ２＞ガロア体除算および＜ステップ３＞ガロア体積和演算の繰り返しによって、ガロア体多項式除算の結果を得る。

【００５５】

【発明の効果】以上のように本発明によれば、ガロア体ベキ乗々回路と、ツリー状に接続されたガロア体乗算器とを備えることにより、回路規模を増大させることなくパイプライン化が可能で、回路規模を増大させることなく複数の原始多項式に対応し、ゲートアレイやＦＰＧＡなどにも容易に実装することが可能なガロア体逆元生成器を得ることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１に係るガロア体逆元生成器の構成を示すブロック図

12

【図２】本発明の実施の形態２に係るガロア体除算器の構成を示すブロック図

【図３】本発明の実施の形態３に係るガロア体演算器の構成を示すブロック図

【図４】本発明の実施の形態４に係るガロア体多項式除算器の構成を示すブロック図

【図５】従来のガロア体逆元生成器の構成を示すブロック図

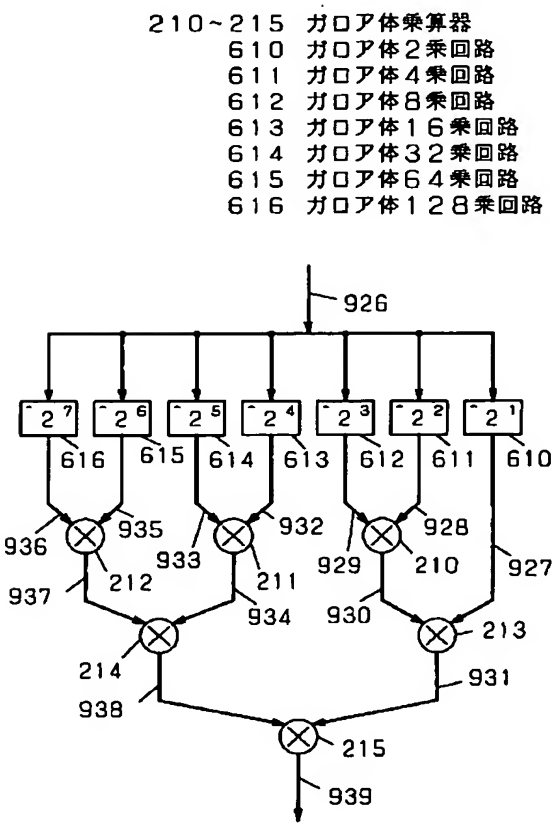
【図６】従来のガロア体除算器の構成を示すブロック図

【図７】従来のガロア体多項式除算器の構成を示すブロック図

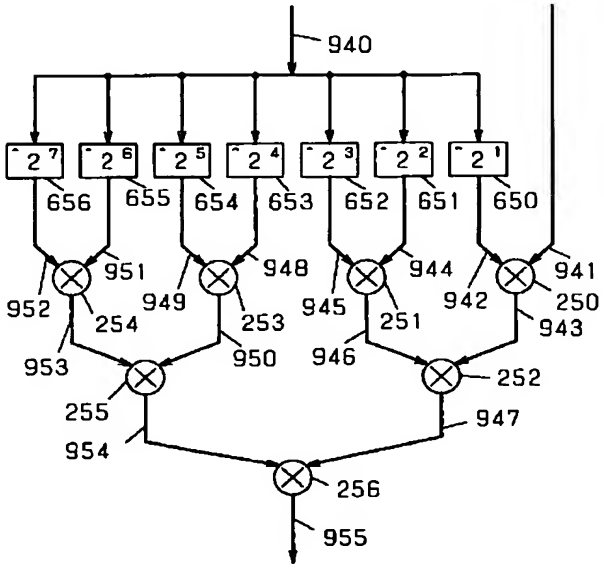
【符号の説明】

２１０～２１５　ガロア体乗算器
６１０　ガロア体２乗回路
６１１　ガロア体４乗回路
６１２　ガロア体８乗回路
６１３　ガロア体１６乗回路
６１４　ガロア体３２乗回路
６１５　ガロア体６４乗回路
６１６　ガロア体１２８乗回路

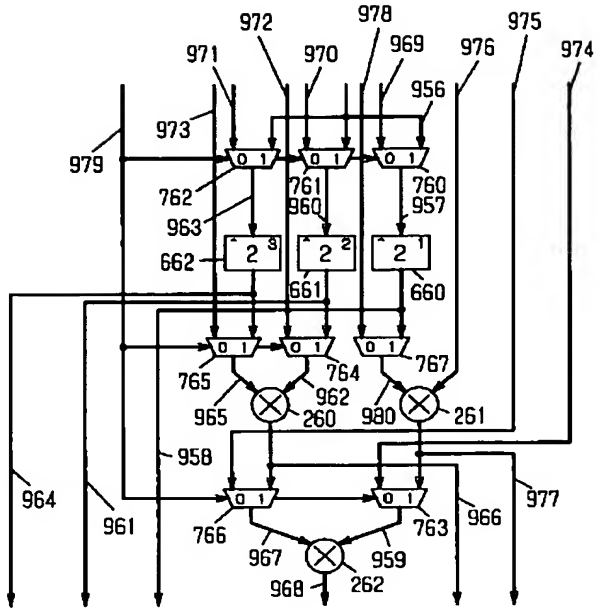
【図１】



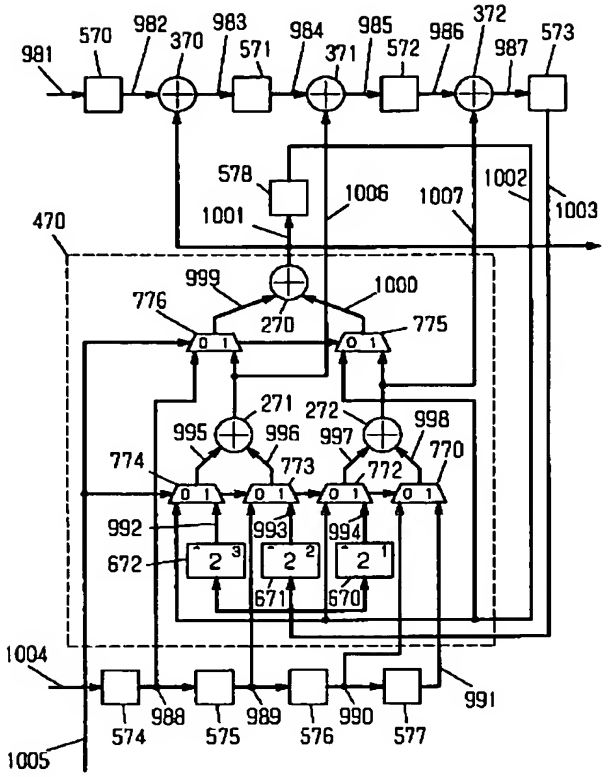
【図２】



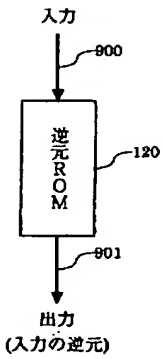
【図３】


972
978
975
971
970
969
976
974
956
973
979
762
761
760
960
957
963
662
661
660
765
764
767
962
965
260
980
261
958
964
961
766
763
966
977
967
959
968
262

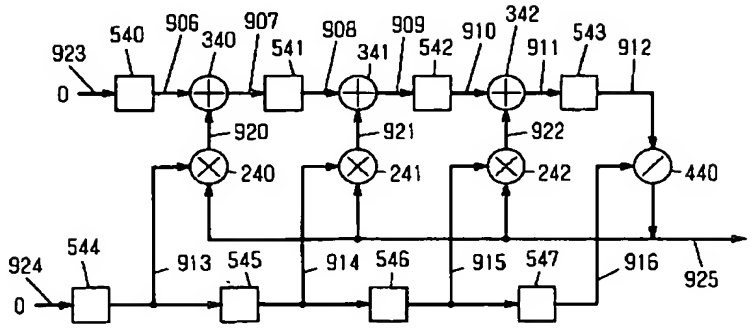
【図４】


981
570
982
370
983
571
984
371
985
572
986
372
987
573
578
1001
1006
1007
1002
1003
470
999
1000
776
270
775
271
272
995
996
997
998
774
773
772
770
992
993
994
672
671
670
1004
988
989
990
991
574
575
576
577
1005

【図５】


入力
900
逆元ROM
120
901
出力
(入力の逆元)

【図７】


923
0
540
906
340
907
541
908
341
909
542
910
342
911
543
912
920
921
922
240
241
242
440
924
0
544
913
545
914
546
915
547
916
925

【図６】